



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|---------------------------|---------------------|------------------|
| 09/879,575 | 06/12/2001 | James Alexander Reeds III | 1999-0275 | 4755 |
| 52218 | 7590 | 11/16/2006 | EXAMINER | |
| ZAGORIN O'BRIEN GRAHAM LLP (037) 7600B NORTH CAPITAL OF TEXAS HIGHWAY SUITE 350 AUSTIN, TX 78731-1191 | | | TRAN, ELLEN C | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2134 | |

DATE MAILED: 11/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/879,575

Applicant(s)

REEDS ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 September 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 and 25-56 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 and 25-56 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is responsive to communication: filed on 27 September 2006 with acknowledgement of an original application filed on 12 June 2001.
2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 27 September 2006 has been entered.
3. Claims 1-22 and 25-56 are currently pending in this application. Claims 1, 14, 33, 41, 48, 49, and 53 are independent claims; claims 2, 4, 10, 17, 25, 36, 44, 49, and 53 have been amended; claims 23-24 have been cancelled, claims 54-56 are new. Amendment to the claims, specification, and drawings are accepted.

Response to Arguments

4. Applicant's arguments filed 23 August 2006 have been fully considered but they are not persuasive where noted below or moot due to new grounds of rejection, see detailed rejection below.

In response to Applicant's argument on page 17, "*Regardless the validity of the Examiner's interpretation, Medvinsky does not disclose or suggest determining if a difference between timestamp or between SSRCs is less than a threshold*". The Examiner disagrees with argument as indicated in paragraph [0034] of Medvinsky the steam cipher is synchronized so that the correct key stream is utilized 'synchronization' inherently is 'determining if a difference between a received session count within a received encrypted data packed and a locally

Art Unit: 2134

generated session count is less than a threshold. In addition paragraph [0035] explains "As used herein a time stamp is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data".

In response to Applicant's argument on page 18, *"Claims 20 and 47 variously recite truncating a session count, while claims 8, 27, 38, and 51 variously recite expanding a session count. Medvinsky fails to disclose or suggest truncating or expanding a session count, a time stamp, or a session source identifier"*. The Examiner disagrees paragraph [0054] of Medvinsky discloses a packet size change this inherently the same as truncating or expanding.

In response to Applicant's argument on page 18, *"Claims 9-13, 28-32, 40, and 52 are rejected under 103 as being unpatentable over Medvinsky in further view of Chang ... It is not clear whether pages 4 and 5 are the fourth and fifth pages ... Applicant respectfully request the Office to identify section of Chang that purportedly support the rejection by column and lines"*. The reference that should have been identified is Staring US Patent Publication No. 2001/0007127, now patent 7,110,546; the section identified is correct page 5, on paragraph 0052, now col. 10, lines 1-30.

In response to Applicant's argument on page 18, *"none of the art of record discloses or suggest truncating a session count or a truncator configured to or expanding a session count, a time stamp, or a session source identifier"*. The Examiner disagrees paragraph [0054] of Medvinsky discloses a packet size change this inherently the same as truncating or expanding.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 4, 17, 25-32, 36, and 44 contain the trademark/trade name Rivest Cipher 4 owned by RSA. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a proprietary standard for stream cipher and, accordingly, the identification/description is indefinite. As discussed previously Rivest Cipher 4 is a trade name it should not be in the claims. The applicant can overcome this rejection by providing a specification of RC4 algorithm. Providing the words RC4 stand for does not overcome the rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2134

8. **Claims 1-8, 14-27, 33-39, 41-51, and 53-56** are rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081) in view of Weidong U.S. Patent 6,819,766 (hereinafter '766).

As to independent claim 1, "A method comprising: selecting ... segment of a continuous decryption key stream based on a received session count of a data packet" is taught in '081 page 3, paragraphs 0033-0034; the following is not explicitly taught in '081:

"a fixed length" however '766 teaches an initial vector which is an obvious variation of fixed length in col. 2, lines 45-48;

"and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" however '766 teaches decrypting data by dividing the data into known lengths (i.e. 'fixed lengths) known only by the party encrypting and party intended to decrypt the data. Decrypting the data packet using the regenerated session key in col. 2, line 45 through col. 3, line 17.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 to include a means to pad the data to form a fixed size for encryption or decryption. One of ordinary skill in the art would have been motivated to perform such a modification because many different approaches are needed to protect data as it is stored and transmitted on computer systems an improvement to these systems is needed that does not require sophisticated infrastructures see '766 (col. 1, lines 12 et seq. and col. 2, lines 29 et seq.). "As confidential and sensitive data is increasingly stored on computer systems, or transmitted over communications networks, including the Internet, it is of increasing

Art Unit: 2134

importance to have methods and systems to ensure the security of such data. Typically, such data is encrypted as it is stored or transmitted by a computer system and then decrypted when the data is to be accessed after being retrieved or received. Many different approaches are known to those skilled in the art and are available to permit users to encrypt and then decrypt computer data ... It is therefore desirable to have a computer system which is capable of encryption key management without requiring a security infrastructure such as a key distribution center or a certificate authority”.

As to dependent claim 2, “wherein the applying comprises performing a bit per bit streaming decryption process” is disclosed in ‘081 page 3, paragraph 0034.

As to dependent claim 3, “wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet” is taught in ‘081 page 3, paragraph 0034.

As to dependent claim 4, “wherein the applying further comprises performing a Rivest Cipher 4 operation with the portion of the fixed length segment and the data packet” is shown in ‘081 page 3, paragraph 0034.

As to dependent claim 5, “further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count” is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claim 6, “wherein the data packet further comprise at least a portion of a received message digest value” is disclosed in ‘081 page 4, paragraph 0054.

As to dependent claim 7 “wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated

session count is less than a threshold value” is shown in ‘081 page 4, paragraphs 0036-0051, note the threshold value inherently is the counter ‘N’ value.

As to dependent claim 8, “wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count” is disclosed in ‘081 page 4 paragraph 0054.

As to dependent claim 54, “further comprising: padding the payload to a given size with padding, the given size corresponding to the fixed length segment size, wherein the fixed length segment of the continuous decryption key is applied to the padded payload, a remaining portion of the fixed length segment being applied to the padding” however ‘766 teaches the final step of adding padding to the encrypted data packet is to add information required for decryption, to decrypt the encrypted data the mapping used with the padded data to encrypt is used for decryption in col. 9, lines 11-40 and col. 7, lines 18-29. The motivation to combine ‘081 and ‘766 is the same as stated above in claim 1.

As to independent claim 14, “A method of generating an encrypted data packet, the method comprising: selecting ... segment of a continuous encryption key stream” is taught in ‘081 pages 3-4 paragraphs 0033-0034; the following is not explicitly taught in ‘081:

“a fixed length” however ‘766 teaches an initial vector which is an obvious variation of fixed length in col. 2, lines 45-48;

“applying a portion of the fixed length segment to data to form an encrypted payload; generating a session count based in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet” however ‘766 teaches establishing an initial vector (i.e. fixed length segment) to form an encrypted session key then reformatting the binary representation interleaved with the session key to form encrypted data (i.e. encrypted payload) in col. 2, lines 45-61.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in ‘081 to include a means to pad the data to form a fixed size for encryption or decryption. One of ordinary skill in the art would have been motivated to perform such a modification because many different approaches are needed to protect data as it is stored and transmitted on computer systems an improvement to these systems is needed that does not require sophisticated infrastructures see ‘766 (col. 1, lines 12 et seq. and col. 2, lines 29 et seq.). “As confidential and sensitive data is increasingly stored on computer systems, or transmitted over communications networks, including the Internet, it is of increasing importance to have methods and systems to ensure the security of such data. Typically, such data is encrypted as it is stored or transmitted by a computer system and then decrypted when the data is to be accessed after being retrieved or received. Many different approaches are known to those skilled in the art and are available to permit users to encrypt and then decrypt computer data ... It is therefore desirable to have a computer system which is capable of encryption key management without requiring a security infrastructure such as a key distribution center or a certificate authority”.

As to dependent claims 15, 16, and 17, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to dependent claim 18, “further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet” is taught in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 19, “wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key” is shown in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 20, “further comprising: forming the at least a portion of the message digest value by truncating the message digest value” is disclosed in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 21, “further comprising transmitting the encrypted data packet to a receiver through a communication channel” is taught in ‘081 page 2, paragraph 0016.

As to dependent claim 22, “further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet” is shown in ‘081 pages 3-4 paragraphs 0033-0034 and page 4, paragraphs 0053-0055.

As to dependent claims 25-27, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to dependent claim 55, **“further comprising: padding the data with padding; applying the fixed length segment to the padded data to form padded encrypted data, wherein a remaining portion of the fixed length segment is applied to the padding; and de-padding the padded encrypted data to form the encrypted payload”** however ‘766 teaches the final step of adding padding to the encrypted data packet is to add information required for decryption, to decrypt the encrypted data the mapping used with the padded data to encrypt is used for decryption in col. 9, lines 11-40 and col. 7, lines 18-29. The motivation to combine ‘091 and ‘766 is the same as stated above in claim 14.

As to independent claim 33, **“A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold”** is taught in ‘081 pages 3-4 paragraphs 0033-0034;

“if the difference is less than the threshold” is shown in ‘081 page 4, paragraphs 0036-0051, note the threshold value inherently is the counter ‘N’ value; the following is not explicitly taught in ‘081:

“and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet” however ‘766 teaches decrypting data by dividing the data into known lengths (i.e. ‘fixed lengths) known only by the party encrypting and party

intended to decrypt the data. Decrypting the data packet using the regenerated session key in col. 2, line 45 through col. 3, line 17.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 to include a means to pad the data to form a fixed size for encryption or decryption. One of ordinary skill in the art would have been motivated to perform such a modification because many different approaches are needed to protect data as it is stored and transmitted on computer systems an improvement to these systems is needed that does not require sophisticated infrastructures see '766 (col. 1, lines 12 et seq. and col. 2, lines 29 et seq.). "As confidential and sensitive data is increasingly stored on computer systems, or transmitted over communications networks, including the Internet, it is of increasing importance to have methods and systems to ensure the security of such data. Typically, such data is encrypted as it is stored or transmitted by a computer system and then decrypted when the data is to be accessed after being retrieved or received. Many different approaches are known to those skilled in the art and are available to permit users to encrypt and then decrypt computer data ... It is therefore desirable to have a computer system which is capable of encryption key management without requiring a security infrastructure such as a key distribution center or a certificate authority".

As to dependent claims 34-39 these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42-51, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to dependent claim 56, “further comprising: a padding engine operable to pad the data and coupled to supply the padded data to the encryption engine; and a pad remover coupled to receive encrypted padded data from the encryption engine and operable to remove the encrypted padding” however ‘766 teaches the final step of adding padding to the encrypted data packet is to add information required for decryption, to decrypt the encrypted data the mapping used with the padded data to encrypt is used for decryption in col. 9, lines 11-40 and col. 7, lines 18-29. The motivation to combine ‘091 and ‘766 is the same as stated above in claim 14.

As to independent claim 48, is directed to a system consisting of independent claims 33 and 41; therefore it is rejected along the same rationale.

As to independent claim 49, “A method comprising: receiving a data packet through a communication channel” is taught in page 2, paragraph 0016;

“the data packet comprising at least a portion of a session count; selecting ... segment of a continuous decryption key stream based on the session count” is taught in ‘081 pages 3-4 paragraphs 0033-0034;
the following is not explicitly taught in ‘081:

“a fixed length” however ‘766 teaches an initial vector which is an obvious variation of fixed length in col. 2, lines 45-48;

“and applying a portion of the fixed length segment by performing a bit per bit streaming decryption to decrypt a payload of the data packet” however ‘766 teaches

Art Unit: 2134

decrypting data by dividing the data into known lengths (i.e. 'fixed lengths) known only by the party encrypting and party intended to decrypt the data. Decrypting the data packet using the regenerated session key in col. 2, line 45 through col. 3, line 37, note the interleaving of the session key which is one byte long (8 bits) into the data, is an obvious variation of a bit by bit streaming decryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 to include a means to pad the data to form a fixed size for encryption or decryption. One of ordinary skill in the art would have been motivated to perform such a modification because many different approaches are needed to protect data as it is stored and transmitted on computer systems an improvement to these systems is needed that does not require sophisticated infrastructures see '766 (col. 1, lines 12 et seq. and col. 2, lines 29 et seq.). "As confidential and sensitive data is increasingly stored on computer systems, or transmitted over communications networks, including the Internet, it is of increasing importance to have methods and systems to ensure the security of such data. Typically, such data is encrypted as it is stored or transmitted by a computer system and then decrypted when the data is to be accessed after being retrieved or received. Many different approaches are known to those skilled in the art and are available to permit users to encrypt and then decrypt computer data ... It is therefore desirable to have a computer system which is capable of encryption key management without requiring a security infrastructure such as a key distribution center or a certificate authority".

As to dependent claims 50 and 51, these claims contain substantially similar subject matter as claims 7 and 8; therefore they are rejected along the same rationale.

As to independent claim 53, **“A method of generating an encrypted data packet, the method comprising: selecting ... segment of a continuous encryption key stream”** is taught in ‘081 pages 3-4 paragraphs 0033-0034;
the following is not explicitly taught in ‘081:

“a fixed length” however ‘766 teaches an initial vector which is an obvious variation of fixed length in col. 2, lines 45-48;

“applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload; generating a session count in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet” however ‘766 teaches decrypting data by dividing the data into known lengths (i.e. ‘fixed lengths) known only by the party encrypting and party intended to decrypt the data. Decrypting the data packet using the regenerated session key in col. 2, line 45 through col. 3, line 37, note the interleaving of the session key which is one byte long (8 bits) into the data, is an obvious variation of a bit by bit streaming decryption.

9. Claims 9-13, 28-32, 40, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘081 in view of ‘766 in further view of Staring U.S. Patent 7,110,546 (hereinafter ‘546).

As to dependent claim 9, the following is not taught in the combination of ‘081 and ‘766: **“further comprising: discarding the data packet if the difference is not less than the threshold value”** however ‘546 teaches “The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the

Art Unit: 2134

retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action" in col. 10, lines 1-30.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 and '766 to include a means to compare the keys being used and take appropriate action (i.e. delete packet) when a match is not found. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to protect data during transmission (see '546 col. 1, lines 51-63). "It is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method. It is an object of the invention to provide a secure communication system, sink device and secure communication method which overcome above mentioned drawback".

As to dependent claim 10, "further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference is not less than the threshold value" is taught in '081 page 4, paragraphs 0041- 0053 "it signals the CODEC change to gateway controller 106. MTA 104 generates a new set of RTP key stream and a new initial time stamp. Herein lies a first advantage of the present invention. The related art provides for re-derivation of the RTP key stream when a CODEC change occurs, by providing the following key derivation function ...

Art Unit: 2134

“End-End RTP Key Change <N>” is a label that is used as a parameter to the key derivation function”.

As to dependent claim 11, **“further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value”** is taught in ‘546 col. 10, lines 1-51. The motivation to combine references ‘081 and ‘546 is the same as stated above in claim 9.

As to dependent claim 12, **“further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value”** is shown in ‘081 page 4, paragraph 4-5, paragraphs 0054-0057 “In a further embodiment, the above solution is employed for a MAC (Message Authentication Code) algorithm change, resulting in a packet size change. Traditionally, for convenience the same RC4 key stream may be used in the generation of the keying material needed to calculate a MAC for each packet (a MAC is appended after the encrypted text). Where the MAC pad is key used to generate the MAC, for one-time use only. So, where a key stream is used for MAC generation (instead of or in addition to encryption) and the size of that random pad changes, one must rekey and start a new RC4 key stream in the same way as for CODE changes”.

As to dependent claim 13, **“further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally**

Art Unit: 2134

generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value” is shown in ‘081 page 4, paragraph 4-5, paragraphs 0054-0057.

As to **dependent claims 28-32**, these claims contain substantially similar subject matter as claims 9-13; therefore they are rejected along the same rationale.

As to **dependent claim 40**, **“further comprising: a message digest extractor configured to extract the at least a portion of the received message digest value from the received encrypted data packet”** is taught in ‘081 page 4, paragraph 0054 **“In a further embodiment, the above solution is employed for a MAC (message Authentication Code) algorithm change, resulting a in a packet size change”;**

“a message digest generator configured to generate a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key” is shown in ‘081 pages 4-5 paragraph 0055-0056 **“For example, additional key stream bytes may be allocated to calculate a MAC for each frame. However, ehre is only one MAC needed for the whole RTP packet and if an RTP packet contains multiple frames only the key stream bytes allocated to one of the frames ...**

Where the MAC pad is a key used to generate the MAC, for one-time use only;

“a truncator configured to truncate the locally generated message digest value to form a truncated message digest; and a message digest evaluator configured to compare the truncated message digest value to the at least a portion of the received message digest value” is disclosed in ‘081 page 5, paragraph 0057 **“one must rekey and start a new RC4 key stream in the same way as fro CODEC changes”;**

“where the received is configured to discard the received encrypted data packed it the truncated message digest value does not match the at least a portion of the received message digest value” is taught in ‘546 col. 10, lines 1-30 “The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action”. The motivation to combine references ‘081 and ‘546 is the same as stated above in claim 9.

As to dependent claim 52, “further comprising discarding the data packet if the difference is not less than the threshold value” is taught in ‘546 col. 10, lines 1-30. The motivation to combine references ‘081 and ‘546 is the same as stated above in claim 9.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is

(571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

Art Unit: 2134

system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ellen Tran
Patent Examiner
Technology Center 2134
31 October 2006